

## **1. Overview**

Email is a mechanism for official communications within the University of Arizona. All employees and students are expected to have an official University email account. Users should follow sound professional practices in maintaining the security and information integrity of email communication.

## **2. Purpose**

The following guidelines will assist those employed or affiliated with the University in safe, secure usage of email and emailing software. These guidelines should not be used to diminish existing college or departmental security procedures.

## **3. Scope**

These guidelines apply to all email users connected to the university network regardless of the email provider.

## **4. Guidelines**

### **4.1. General email usage**

Email is a vital tool in day-to-day operations and with a little education and awareness can be a safe means of communication. Users should learn what to look for and how to avoid becoming victims and take all necessary precautions to protect themselves. It is important to be aware of the following points when communicating via email:

### **4.2. Scams and Spam**

An increasingly common type of scam using spam is phishing. Phishing attacks use 'spoofed' e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. Emails can be forged, including the send and return address, the email body, and other email information.

### **4.3. Steps for Prevention**

- Treat all email with suspicion.

- Be cautious when using a link in an email to get to a web page. If you must visit the website, type the URL directly into your browser's address bar.
- Never send personal or financial information to anyone via email.
- Regularly scrutinize bank, credit and debit card statements to ensure that all transactions are legitimate. If anything looks suspicious, contact financial institutions or card issuers.
- Make sure that software has all security updates installed.
- Ensure that you have adequate safeguards against fraud before accessing financial information online – Contact your financial institution for information.

#### **4.4. Email Security Concerns**

- Beware of all attachments. Only open those that you are expecting from a bonafide source or have confirmed with the sender.
  - ✓ The Know test: Is the email from someone that you know?
  - ✓ The Received test: Have you received email from this sender before?
  - ✓ The Expect test: Were you expecting email with an attachment from this sender?
  - ✓ The Sense test: Does email from the sender with the contents as described in the Subject line and the name of the attachment(s) make sense?
  - ✓ The Virus test: Does this email contain a virus?
- Beware of software updates sent by email! Corporations and financial institutions will never send any security patches, updates, distributions or other executable files by email – they'll send notifications instead.
- Beware of URL's within an email message. Best practice is to open the browser and type in the URL rather than click it from within the email message.
- Use email filters to move identified suspected spam mail to a spam folder for later verification.

#### **4.5. Email spoofing**

Email spoofing may occur in different forms, but all have a similar result: a user receives email that appears to have originated from one source when it actually was sent from another. Email spoofing is often an attempt to trick the user into releasing sensitive information (such as passwords), or making a damaging statement. Spoofed email can range from harmless pranks to social engineering ploys.

Examples of spoofed email that could affect security include:

- Email that appears to come from a known source but contains a virus or other malicious code or instructions.
- Email claiming to be from a system administrator requesting users to change their password to a supplied word or phrase and/or threatening to suspend their account unless they comply.

- Email claiming to be from a person in authority requesting users to send them a password or other sensitive information.

If someone can obtain the username and password used to access an email account, they can read and send email messages impersonating the user of that account.

It is very easy to construct messages that appear to be from someone other than who they are actually from. Many viruses use this method to propagate themselves. In general, there is no simple way to be sure that the apparent sender of a message actually sent it.

Note that while service providers may occasionally request that users change their password, they usually will not specify what a password should be changed to. Legitimate internet service providers will never ask users to send any personal information via email. If it is suspected that an email is spoofed by someone with malicious intent, contact the internet service provider's support personnel immediately.

#### **4.6. Email-borne viruses**

Viruses and other types of malicious code are often spread as attachments to email messages. Before opening any attachments, verify the source of the attachment. It is not enough that the mail originated from a recognized address. For example the Melissa virus spread because it originated from a familiar address. Also, malicious code might be distributed in amusing or enticing programs.

Only run programs that are created by a trusted person or company. Forwarding programs of unknown origin to your friends or coworkers simply because they are amusing -- could spread a worm or Trojan horse.

#### **4.7. Hidden file extensions**

Windows operating systems contain an option to "Hide file extensions for known file types". The option is enabled by default, it is recommended users disable this option in order to have file extensions displayed by Windows. (See your systems administrator for assistance.) Multiple email-borne viruses are known to exploit hidden file extensions. Examples include:

Downloader (MySis.avi.exe or QuickFlick.mpg.exe)  
VBS/OnTheFly (AnnaKournikova.jpg.vbs)

The files attached to the email messages sent by these viruses may appear to be harmless text (.txt), MPEG (.mpg), AVI (.avi) or other file types when in fact the file is a malicious script or executable (.vbs or .exe, for example).

#### 4.8. General email clients

There are many email clients available for use. It is important to understand features of email clients when making a choice. Clients need to be securely configured and kept current with the latest patches. Here is a list of commonly used clients, please refer to vendor's website for information.

- Microsoft Outlook
- Apple Macintosh Mail
- Eudora
- Microsoft Outlook Express
- Thunderbird/Mozilla/Netscape
- Lotus Notes
- UA Webmail

Note: If the connection to a WebMail server is "insecure" (i.e. the address is http:// and NOT https://), then all information including username and password is in plain text as it passes between the WebMail server and the computer and is subject to hijacking.

All *italicized terms* used in this standard are defined in the Information Security Terms Guideline.

#### IX. Related Guidance

Information Security Terms Guideline (IS-G100)

#### Revision History

Initial Draft	5/25/06
Effective Date	5/27/08